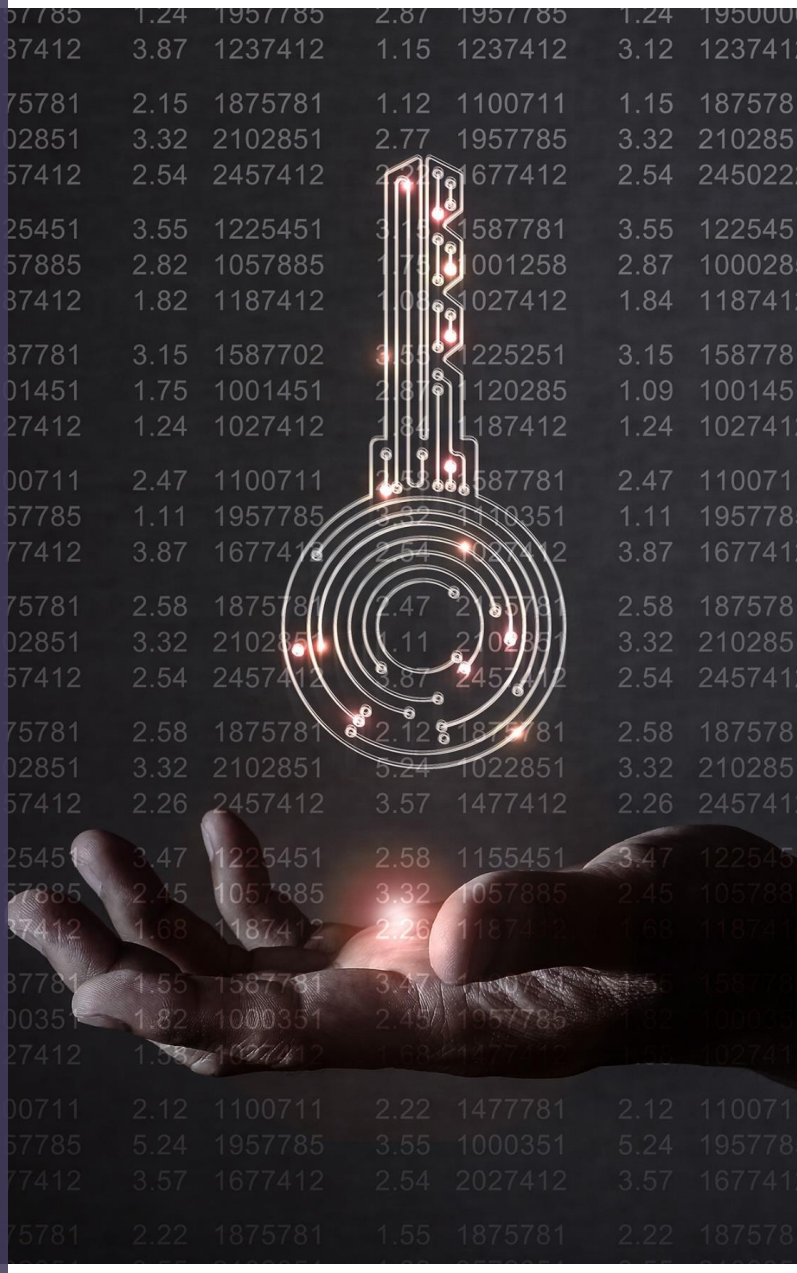
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

AUGUST 2020

NEWS

Penti Clothing Industry and Trade Co. and Its Subsidiaries Data Breach Notification

It has been notified by Penti Clothing Industry and Trade Co. and Its Subsidiaries, which has the title of data controller, to the Authority about the data breach occurred as a result of a ransom attack on the systems. It was determined that the data breach occurred on 31.07.2020, on the same date.

It was determined that nearly 45,000 data of Penti Clothing Industry and Trade Co. and Its Subsidiaries were leaked as a result of the attack. In addition, it has been stated that the affected personal data categories affected by the data breach are identity, contact and customer transaction details, the investigations are ongoing by Penti and the number of people affected by the data breach has not been determined yet and.

The aforementioned violation was published on the website of the Authority on 06.08.2020 and the related investigation continues.

Barilla Gıda A.Ş. Data Breach Notification

It has been notified to the Authority by Barilla Gıda A.Ş. that, according to the data breach occurred on 12.08.2020, it has been stated that with a cyber-attack, the disks and files are made inaccessible by running the ransomware, the content of the affected data and personal data, the relevant data subject groups and the number of people cannot be determined, according to the notification of the ransomers and the investigation of the IBM, up to 4 GB of data has been leaked.

The aforementioned data breach was published on the website of the Authority on 18.08.2020 and the investigation is ongoing.

Turkish Personal Data Protection Authority published a public announcement regarding the Introduction Form for Data Controllers

Turkish Personal Data Protection Authority ("Authority") published a public announcement regarding the "Introduction Form for Data Controllers" on 12.08.2020.

"Introduction Form for Data Controllers" ("Form") has been sent by the Authority during the supervision made within the scope of Article 15 of KVKK and requested it to be filled in and submitted to the Authority along with the requested information and documents.

In the announcement, it was stated that this Form was not filled or was found to be incomplete in the supervision made as a result of some complaints and notices. The Authority emphasized that the due sensitivity and care should be exercised in filling the form completely and submitting it to the Authority.

Kariyer.net Data Breach Notification

According to the letter sent to the Authority by Kariyer.net Electronic Publishing and Communication, which has the title of data controller, it has been stated that the data breach occurred on 10.08.2020 and was detected on 12.08.2020 by a consultant serving as a supplier to Kariyer.net by informing an employee of Kariyer.net that a file allegedly belonging to 50,000 members of the said website was uploaded to a website on the same day. The number of people affected by the breach is 40.955 and the affected data are e-mail address, user password, name and surname, date of birth, phone number, profile photo, URL link information, city of residence, district of residence.

The aforementioned data breach was published on the website of the Authority on 18.08.2020 and the investigation is ongoing.

Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği Data Breach Notification

Dap Rotana Dalga ve Vazo Rezidans Toplu Yapı Yöneticiliği, which has the title of data controller, sent a data breach notification to the Authority. In summary, it was stated that the personal data were shared with third parties by an employee, the data breach occurred on 05.03.2020 and as a result of a company report, received on 13.08.2020, the breach was detected. Identity, communication, location and legal transaction data categories of the violated persons were seized. It was stated that the number of persons affected by the violation was 2328.

The aforementioned violation was published on the website of the Authority on 18.08.2020 and the investigation is ongoing.

Rezzan Günday (Şimşek Pharmacy) Data Breach Notification

In the letter sent to the Authority by Rezzan Günday (Şimşek Pharmacy), who has the title of data controller, it has been stated that a former employee of the data controller obtained the ID numbers of the patients by taking a screenshot with a mobile phone and writing them down on paper in order to be able to acquire medicine from different pharmacies. In addition, medicines were acquired by using the identification numbers obtained during the pandemic period over the "Continuation Prescription" application. As a result of all these, a data breach has occurred.

It has been stated that the data breach has continued since October 2019 and appeared on 11.08.2020. It has been determined that the personal data of the patients affected by the breach are T.R. identity number, telephone number, patient status, institution name (General Directorate Of Social Security Organization For Artisans And The Self-Employed, SSI, 60/G Insured) and also sensitive personal data (health information) are included in the data breach. Although the number of people affected by the violation is not known, it has been stated that a criminal complaint has been made to the Public Prosecutor's Office about the incident subject to the breach.

The aforementioned data breach was published on the website of the Authority on 18.08.2020 and the investigation is ongoing.

What Is Brought with the Identity Sharing System Regulation?

The Regulation on the Identity Sharing System Regulation ("Regulation") published in the Official Gazette on 21.08.2020 regulates the sharing of the information in the database of the General Directorate of Civil Registration and Citizenship of the Ministry of Interior with the recipient institutions. The recipient institution as defined in the Article 4 of the Regulation refers to: "Other public institutions and organizations other than the General Directorate benefiting from the Identity Sharing System". In accordance with the Article 5 of the Regulation titled "Sharing Principles", the sharing with the recipient institutions will be made within the framework of KVKK and the related procedures and principles in the secondary regulations of KVKK.

The Regulation also includes provisions regarding the purpose of data processing and legal basis for the data to be shared with the recipient institutions, that the institutions are obliged to use the data they obtain for a limited purpose and to ensure the data is up to date

System authorization, definitions and procedures and principles regarding the use of the system are also specified in the regulation. The confidentiality of the data to be obtained through the system is regulated in the Article 9 of the Regulation and with this Article, the obligation to ensure data security is imposed on the recipient institutions. In the continuation of the related article, it is stated that the provisions regarding the privacy of private life and the protection of personal data will be taken as basis in the use of the system, and KVKK will be applied especially in technical and administrative measures to be taken. Finally, it has been stated that at the point of processing and storing personal data the General Directorate's obligations will be fulfilled as specified in KVKK.

The Danish Data Protection Authority Fined Privatbo 150.000 DKK for the Unintentional Disclosure of Personal Information

The Danish company PrivatBo helped a housing fund to sell three properties in 2018. On this occasion, PrivatBo provided materials which have been distributed to residents with a total of 424 USB keys about the properties. However, PrivatBo was unaware that some of the documents distributed with these USB keys contained confidential personal information that should not be disclosed.

The Danish DPA found that PrivatBo did not comply with the requirements of the Article 32 of the GDPR coinciding with clauses on implementation appropriate technical and organizational security measures in its supervision. Depending on the nature of the case, the Authority chose to notify PrivatBo to the police for the unintentional disclosure of personal information and fined 150.000 DKK.

Administrative Fine for Rælingen Municipality by the Norwegian Data Protection Authority

The Norwegian Data Protection Authority imposed an administrative fine of 47.500 EUR on the Municipality of Rælingen. The fine was imposed after processing data on the health of children with special needs using the digital learning platform Showbie. After further investigation of the case, the Norwegian Data Protection Authority revealed that the security level of the application was not proportionate to the risk and stated that the issue was an extremely important and sensitive as it relates to personal data relating to both children and health.

About the Infringement

The violation affects 15 children with special needs. The Showbie application has been used to transfer personal health data between schools and children's homes.

The Authority determined that the necessary risk and data protection impact assessments and tests have not been completed before the application is put into use. It has been also stated that the absence of security measures when logging into the application made it possible users to get information about the other children in the group.

Following the data breach notification, the Municipality pointed out that there was no indication that any of the children actually suffered material or moral damage, but the Authority did not emphasize this when considering the case. This is because, regardless of whether the risk manifests itself in the form of more substantial damage to the affected children, the violation itself is discovered to be a risk.

The Authority chose to lower the penalty amount after a general assessment based on an investigation from the municipality of Rælingen. An assessment was also made regarding previous practices under the former law. The case was not appealed, and a decision was made at 47.500 EUR.

The Spanish Data Protection Authority (AEPD) Imposed a fine of 70.000 EUR to XFERA MOVILES for Disclosing a Customer's Personal Data to a Third Party

When a Masmovil customer saw personal data of another customer which are the name, surname, identity card number and personal phone number on the invoice received, he notified the relevant customer about the issue. The relevant customer made a complaint to the Authority after this notification and became a plaintiff. After the breach occurred, Masmovil called the data subject and stated that they would monitor the case closely and take the necessary measures as soon as possible.

As a result of the investigation, the Authority has determined that Masmovil's confidentiality principle in the Article 5/1(f) of GDPR has been violated. XFERA MOVILES, a subsidiary of the Masmovil group of companies, was imposed a fine of 70.000 EUR.

Spanish Data Protection Authority (AEPD) Imposed A Fine to Vodafone Spain of 75,000 EUR

Although the Data Subject exercised his right to erasure in 2015, he became a plaintiff for receiving advertising SMS's and his phone number was being used for marketing purposes. As a result of the investigations, the Authority imposed a fine of 75.000 EUR to VODAFONE ESPAÑA.

The Data Controller stated that staff used this number as a "dummy number", as the plaintiff's number was easy.

The Authority decided that VODAFONE ESPAÑA violated Article 6/1 of the GDPR by processing the plaintiff's personal data without any legal basis.

Spanish Data Protection Authority (AEPD) Imposed a Fine of 1200 EUR for the Company for Ad Search to Data Subject Without Consent

A company made offers to a data subject about hotels, ignoring their presence in the advertisement exclusion system. The data subject has used his right to object to data processing for marketing purposes within the scope of Article 21 of the GDPR by being included in this advertisement exclusion system. The company violated its obligation to consult the advertisement exclusion system to prevent the processing of data subjects' personal data who object the marketing calls before making a marketing phone call. As a result of the violation, the company was imposed a fine of 1.200 EUR by the authority.

It was determined that the call was made to data subject from the data controller's number. It was stated that during the call, the data controller informed the data subject that they received their phone number by a friend so that they were presented with a hotel coupon, the names of other friends and information about their participation in the promotion were also given.

The Authority found that this was a violation of Article 48/1(b) of the Spanish General Telecommunications Law of 9/2014.

Belgian Data Protection Authority Fined Proximus 20.000 EUR For Several Various Data Protection Breaches During the Processing of Personal Data For The Purpose of Publishing Public Phone Directories

Facts

A Citizen (plaintiff) requested Proximus, the publisher of a public directory, to withdraw his personal data from being published in Proximus's public directory and the personal data from being published in the directory of other publishers. As the publisher of the directory, Proximus had confirmed that it would no longer publish personal data against the plaintiff and would also notify other publishers not to publish the plaintiff's personal data. However, a few months later, the plaintiff discovered that his personal data was published not only in the Proximus directory, but also in other publisher of a public directory.

Decision of the Litigation Chamber

The litigation Chamber of the Authority confirmed to below along with other points:

Since Proximus publishes its own directory, it should be considered as a data controller due to the data processing activities involved. Therefore, Proximus has a responsibility to align the withdrawal of consent with the actual processing activities.

In this context, Proximus has not taken appropriate measures to ensure and prove that the personal data of the complainant were not unlawfully processed after the withdrawal of consent. Proximus has therefore not fulfilled its obligations as a data controller and therefore violated the Article 6 of the GDPR and Articles 24 and 5(2) of the GDPR, along with Article 7 of the GDPR.

Illegal and discriminatory methods used by Dutch Tax and Customs Administration

The Tax and Customs Administration's Aid Office has processed the nationality information of dual citizens applying for childcare allowance for many years. According to the Data Protection Authority's research, this practice is illegal and discriminatory and is a violation of the GDPR.

It was determined that about 1.4 million people were still registered as dual citizens in the systems of the Tax and Customs Agency in May 2018, which should have already deleted data on dual citizenship in January 2014. However, under the related legislation, dual citizenship should not play a role in the evaluation of childcare benefit applications. Besides, the Tax and Customs Agency has also processed the nationality data of applicants for childcare benefits to combat organized fraud, although this is not necessary for the purpose. Finally, the Tax and Customs Administration used applicants' nationality (not Dutch / Dutch) as an indicator in a system that automatically identifies certain situations as risky, but under the related legislation, it is illegal to use Citizenship data to evaluate applications, combat fraud, and identify risk.

Discriminatory Data Processing

In the Netherlands, the right to childcare allowance depends on the legal residence, not citizenship. Besides, under the GDPR, data processing should not infringe any fundamental rights. Since this fundamental rights include the right to equality and non-discrimination, the Tax and Customs Administration violated the GDPR with the discrimination based on nationality.

The representative of the Authority has stated as in the following, "Our investigation shows that the Tax and Customs Administration's Benefits Office stored and used large amounts of data in various ways over a long period that was entirely impermissible. The specific consequences this has had for individual applicants is beyond the scope of this investigation. However, we know that the nationality or dual nationality of applicants was consistently and systematically used against them, and it should not have been."

Further Steps

The next step is for the Authority to decide whether to impose a sanction, such as a fine, on the Tax and Customs Administration. Prior the decision is made; the Minister of Finance has the first official right to respond to the investigation. Following this, the Data Protection Authority can announce any sanctions it decides to implement in late 2020.

CNIL Fined the Spartoo Which Recorded the Phone Calls Made with Customers for Employees' Training

CNIL, the data protection authority of France, issued fine of EUR 250.000 to Spartoo for violating various articles of the GDPR.

Spartoo provides online shoe sales service to different countries in Europe. Since the data processing within the scope of service affects the data subjects resident in other European countries, CNIL conducted its supervision by triggering cooperation mechanism with other supervisory authorities, in other words data protection authorities, in accordance with GDPR. Thus, the decision is the first decision of CNIL as a lead supervisory authority. Details of the decision are as follows:

CNIL found that Spartoo violated data minimization principle, storage limitation principle, information and data security obligations of GDPR.

CNIL first ruled that permanent recording of phone calls with customers for employee training is contrary to the principle of data minimization stipulated in the Article 5/1(c) of GDPR. Authority found that a weekly wiretapping for each employee does not justify this processing and recording the customers' bank account details when the order was placed over the phone was also excessive. In addition, CNIL found that the collection of customers' health cards was excessive in order to prevent fraud and violated data minimization principle.

CNIL found that Spartoo did not set a data retention period for the data of its customers and prospects, nor did regular erase and archive the data of people who have not logged into their accounts for a long time. The authority also decided that keeping customers' names and passwords for more than 5 years in order for customers to reuse their accounts was not proportionate to the purpose and contradicted the storage limitation principle stipulated in Article 5/1(e) of GDPR.

CNIL found that the customers were misinformed about the legal basis of the processing and that the information provided indicates the legal basis of processing is consent while there was processing for other legal basis. It stated that the legal basis of all processing activities is shown as an explicit consent in the Spartoo' privacy notice, whereas processing is also based on other legal bases. Authority also ruled that the employees were not sufficiently informed about the data processing related to phone calls made with the customers and they were not informed about their rights. CNIL, therefore, decided that Spartoo violated the Article 13 of GDPR.

CNIL concluded that Spartoo did not require customers to use strong enough passwords to access their accounts, thus was in breach of its obligation to ensure data security.

Taking into account more than 3 million customers and more than 25 million prospects affected by the breach, CNIL imposed 250.000 EUR fine on Spartoo and ruled that it complies with GDPR within 3 months and pays 250 EUR per day in case of delay.

The Pilot Project of the South Wales Police Service ("SWP") Was Challenged Regarding the Lawfulness of the Use of Automatic Facial Recognition Technology ("AFR")

AFR is a new technology used to assess whether two face images depict the same person. The AFR type in question, known as AFR Locate, works by extracting faces captured in a live stream from a camera and automatically comparing them with the faces in the watch list. When the collected data is assessed, if there is no match, the captured face image is automatically deleted. In the event of a match, as a result of the alert notification sent, the personnel responsible for AFR use will review the images to decide whether an intervention is needed.

Edward Bridges, a civil liberties campaigner and living in Cardiff, who filed an appeal, also got the support of the Civil Liberties membership organization Liberty. Mr. Bridges was near two AFR Locations, the first on Queen Street in downtown Cardiff on December 21, 2017, and the second at a Fair held at the Motorpoint Arena in Cardiff on March 27, 2018. Bridges was not included on the police watch list at AFR locations, but, given its proximity to cameras, claimed that his footage was recorded by AFR even if it was immediately deleted. South Wales Police Force did not raise any objections. Bridges applied for judicial review on the grounds that AFR is not in compliance with the right to respect for private life under the Article 8 of European Convention on Human Rights (“Convention”), data protection legislation and Public Sector Equality Duty (“PSED”) under the Section 149 of Equality Act 2010.

On September 4, 2019, the Divisional Court dismissed Bridges' claims for judicial review on all grounds. Divisional Court found that the AFR application is in the scope of right to privacy under Article 8 of Convention, but the interference with the rights was lawful and proportionate. Divisional court rejected data protection claims made under the Data Protection Act 1998 and the Data Protection Act 2018 ("DPA 2018").Finally, Bridges argued that AFR does not consider the possibility of producing indirectly discriminatory results on the basis of gender and / or race, thus violating the Public Sector Equality Duty (PSED), as it produces a higher rate of positive matches for women.

Bridges appealed the court's decision on five grounds, and the Court of Appeal (“The Court”) decided unanimously.

The appeal was successful on Ground 1, that the Divisional Court made a mistake as a result of the South Wales Police Force interference with the rights of Bridges in Article 8(1) of the Convention as "accordance with the law" under Article 8(2) of the Convention. The court decided that although the legal framework consists of DPA 2018, the Surveillance Camera Code of Practice and local policies announced by the Police Service, there is no clear guidance on where the AFR can be used and who can be put on the watch list.

The appeal failed on Ground 2 that the Divisional Court made a mistake in determining that the South Wales Police Force's use of the AFR was a “proportionate interference” with Article 8 rights under Article 8 (2). The Court of Appeal conducted an analysis, on one side of the expected benefits of AFR, and on the other, the negative impact of AFR on Bridges. According to this analysis the Court found that the potential benefits were quite large, while the impact on Bridges was quite small and thus the use of AFR was found to be proportional under Article 8 (2).

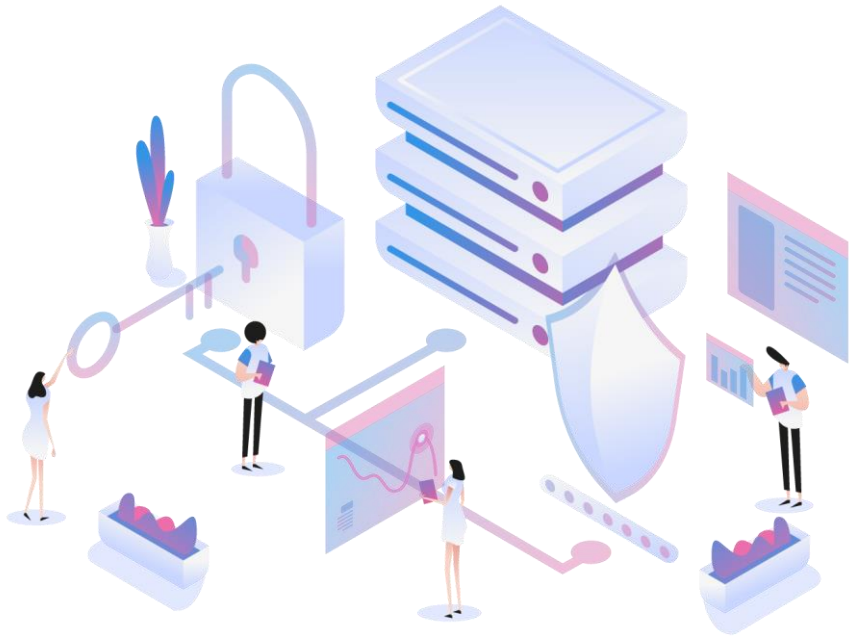
The appeal was successful on Ground 3 that the Divisional Court found it wrong to decide that the South Wales Police Force provided a "data protection impact assessment" ("DPIA") as required by section 64 of DPA 2018.

The appeal failed on Ground 4 that the court of appeal was wrong to not come to a conclusion as to whether the South Wales Police Force implemented an "appropriate policy document" under the section 42 DPA 2018. The Court of Appeal found that the Divisional Court was justified in not reaching a conclusion because the registrations at the two AFR deployments that underpin Bridges' claim occurred before DPA 2018 went into effect.

The appeal was successful on Ground 5. That the Divisional Court is erroneous in accepting that the South Wales Police Force complies with the Equality Obligation in the Public Sector (PSED). The Police Department made a mistake by not taking reasonable steps to question whether the AFR software was racial or gender biased. However, the Court of Appeal noted that there was no clear evidence that the AFR software was actually biased on grounds of race and / or gender.

Data Breach by the Danish Data Protection Authority ('Datatilsynet') Itself on 20th August 2020

The Danish Data Protection Authority ('Datatilsynet') announced a personal data breach on August 20, 2020. It was learned that some of the paper waste containing confidential and sensitive information about citizens and employees and that should have been fragmented was disposed as ordinary paper waste. The Authority noted that this type of material is usually stored electronically in their systems but is printed by the Authority employees when they need to discuss a topic internally. The Authority stated that instead of shredding the papers when employees were done with them, they threw them into the trash, an employee discovered that these papers were disposed as ordinary waste, which means the paper waste is diverted for normal recycling. Additionally, Datatilsynet stated that the personal data security breach was notified to the Authority almost 24 hours late from the 72 hours requirement for the notification of the data breach. The employee responsible for reporting the data breach in question was imposed a penalty of a reprimand. Finally, Datatilsynet stated that it has addressed the issue of notification of affected data subjects, has reviewed all procedures for disposal of wastepaper and tightened its internal guidelines.



INFORMATION GUIDE

The Relation Between Electronic Messages and KVKK

As per the scope of the Law No. 6563 on the Regulation of Electronic Commerce (“Law”) and the Regulation on Commercial Communication and Electronic Commercial Messages ("Regulation"), the procedures and principles for commercial communication with recipients in electronic environment are set out. The legislation also includes essential regulations in terms of personal data.

In accordance with the Article 10 of the Law titled "Protection of Personal Data", the service provider or intermediary service provider is responsible for the security of the data obtained due to the transactions covered by the Law. Personal data cannot be transferred to third parties or used for other purposes without the consent of the data subject.

A similar regulation is also brought with the Article 12 of the Regulation titled "Protection of Personal Data". According to this article, the service provider or intermediary service provider is responsible for the preservation of the personal data obtained due to the services provided within the framework of the Regulation and for taking the necessary measures to prevent illegal access to personal data and processing it. Prior consent should be obtained from the data subject for sharing, processing and using personal data for other purposes.

The Law on The Protection of Personal Data ("KVKK") will be applied for the necessary measures to be taken for the personal data specified in the Law and Regulation and the approvals to be taken from the data subjects.

One of the most concerning issues in practice is the approvals to be obtained from the data subjects mentioned in the provisions above. When sending e-messages or managing such sending activities, personal data processing activity in the context of KVKK will be in question, and personal data collected for e-message sending can be used for other purposes such as conducting marketing and analysis activities. This situation will also require compliance with KVKK along with the Law and Regulation.

As per the scope of the Law No. 6563 on the Regulation of Electronic Commerce (“Law”) and the Regulation on Commercial Communication and Electronic Commercial Messages ("Regulation"), the procedures and principles for commercial communication with recipients in electronic environment are set out. The legislation also includes essential regulations in terms of personal data.

As it is known, there are two types of recipient approval in commercial messages under the Law. While messages sent to merchants and tradesmen can be sent with the option of opt-out without prior approval, a pre-approval (opt-in) is required for individual recipients. The existence of consent or other processing conditions to be obtained in terms of KVKK is interpreted separately according to two types of recipient approvals below.

Personal Data Processing Conditions for Commercial Messages for Merchants-Tradesmen

Although electronic commercial messages can be sent to merchants and tradesmen without prior approval, in the messages to be sent, various personal data such as name, surname, workplace name and address, telephone number of the persons may be processed. In such case, one of the conditions for processing personal data within the scope of KVKK must be met.

Basically, there are two situations likely to be encountered:

*1.Sending the message to be sent to merchants or tradesmen to contact addresses belonging to the legal entity that **do not make** the natural person specific or identifiable*

In this case, sending a marketing e-mail about your logistics service to an address that will not be associated with a natural person will not be covered by KVKK and thus, no legal obligation will arise.

*2.Sending the message to the merchants or tradesmen to the contact addresses that **make** the natural person specific or identifiable*

In this case, for example, when an e-mail is sent to the e-mail address of the authorized person of the company, KVKK compliance will be required in terms of processing personal data. In this case, the concrete situation should be evaluated, and the appropriate processing condition should be determined. For example:

• If the data is publicized in terms of processing activity, the message can be sent,

• If the contractual relationship exists and the e-mail can be considered as being directly related to the execution of the contract, the message can be sent,

• A balance test will be performed for the content of the message and the personal data processed, and if legally appropriate, it can be sent within the scope of legitimate interest,

• If the processing cannot be evaluated within the scope of these processing conditions, it will be necessary to obtain explicit consent in the context of KVKK according to the method of obtaining it.

Personal Data Processing Conditions for Commercial Messages for Individual Recipients

In the messages sent to individual recipients, there will be a data processing activity within the scope of KVKK and data processing conditions will need to be evaluated. In this context, we are in the opinion that there are basically two types of processing conditions:

•Legitimate interest if legally appropriate by performing a balance test for message content and personal data processed,

•Explicit consent, if legitimate interests exceed the limits.

What Are the Methods to Obtain Explicit Consent for e-Messages within the Framework of KVKK?

The explicit consent to be obtained within the scope of KVKK should be related to a specific subject, the minimum elements should be based on the information specified in the relevant legislation and it should be given with free will. In practice, it is seen that two concerns frequently arise for KVKK consent obtained through e-messages:

• If the consent is obtained in a common text with the e-message confirmation text, the principle of "clarity" of the consent to be obtained regarding personal data is damaged. Such that, the consent statements to be obtained regarding the processing of personal data must include a specific subject, be specific in terms of purpose, activity and data, and must be taken separately for each purpose. To be based on a single consent to send an e-message along with the processing of personal data in a common text may damage the consent for personal data in terms of clarity.

• If consent is obtained separately from the e-message confirmation text, this time, e-mails will not be sent to those who do not give their explicit consent but give an e-message approval. This situation, which creates a logical contradiction, will bind explicit consent to another service condition (related to e-mail sending) and will damage the consent for personal data. In this regard, it may damage the quality of giving consent with free will and create a logical contradiction.

In order to minimize concerns, it seems appropriate to obtain the consents by meeting the explicit consent conditions within the scope of KVKK with a common statement. In other words, the elements of explicit consent included in KVKK should be provided, and in order not to damage the principle of clarity, the approval text should only be about the e-message sending permission. For additional data processing activities other than e-message sending confirmation, such as processing message permissions within the framework of the loyalty program, separate explicit consent should be taken.

The point to be considered here is that it is necessary to inform the person in detail about the consequences that will be encountered if the person does not give consent. After all, it should not be forgotten that the ultimate goal of explicit consent is to ensure that the data subjects have a definite right on their data. For this reason, the information to be made while obtaining the consent declaration should include the negative consequences that will be encountered when the consent is given or not, and should be able to give a clear and certain answer to the question "What will happen to my data?"

Processing for Purposes Other than the Activity of Sending E-Message and Explicit Consent

The explicit consent to be obtained in this regard, should obviously be obtained from the data subjects separately from other approvals, within the procedures and principles in accordance with KVKK.

Rabia Dağcı | Legal Consultant | Attorney | CIPP/E

Technical Measure: Labeling and Classification

According to the Article 12/1 of KVKK, data controllers have to take all necessary technical and administrative measures in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data are stored in accordance with the law.

These measures are elaborated in the Personal Data Security Guide published by the Authority and specified at the notification stage to VERBIS.

One of these measures is to take extra security measures for personal data transferred on paper and the relevant documentation should be sent in a “classified/confidential paper” format.

For the protection of sensitive data, it should be known exactly which data to be protected is. For example, sensitive personal data should be included in the "Strictly Confidential Data" category and the data should be kept under control. The most important way to determine this is to use information classification processes.

Organizations should set out the conditions under which they will protect their information assets. In this context, separating the information assets in the Organization according to their degree of confidentiality and specifying the labeling practices provides great contribution to the Organizations.

Controls should be introduced to see if documents with personal data are be left unsurveilled or not. In this regard, Policies on Access to and Use and Classification of Information should be implemented to use in order to provide control of information and documentation containing personal data.

With the information classification and labeling practices, constant awareness of information security within the Organization is provided and the employees are ensured to act consciously on this issue.

Although it seems that the measure of "extra security measures to be taken for personal data transferred on paper and the relevant documentation to be sent in a classified/confidential paper format" specified at the declaration stage to VERBIS seems to be realized by adding the phrase "CONFIDENTIAL" to physical documents and restricting access to documents containing sensitive data, one of the most important processes in information classification and labeling is to protect the data we obtain by digital means.

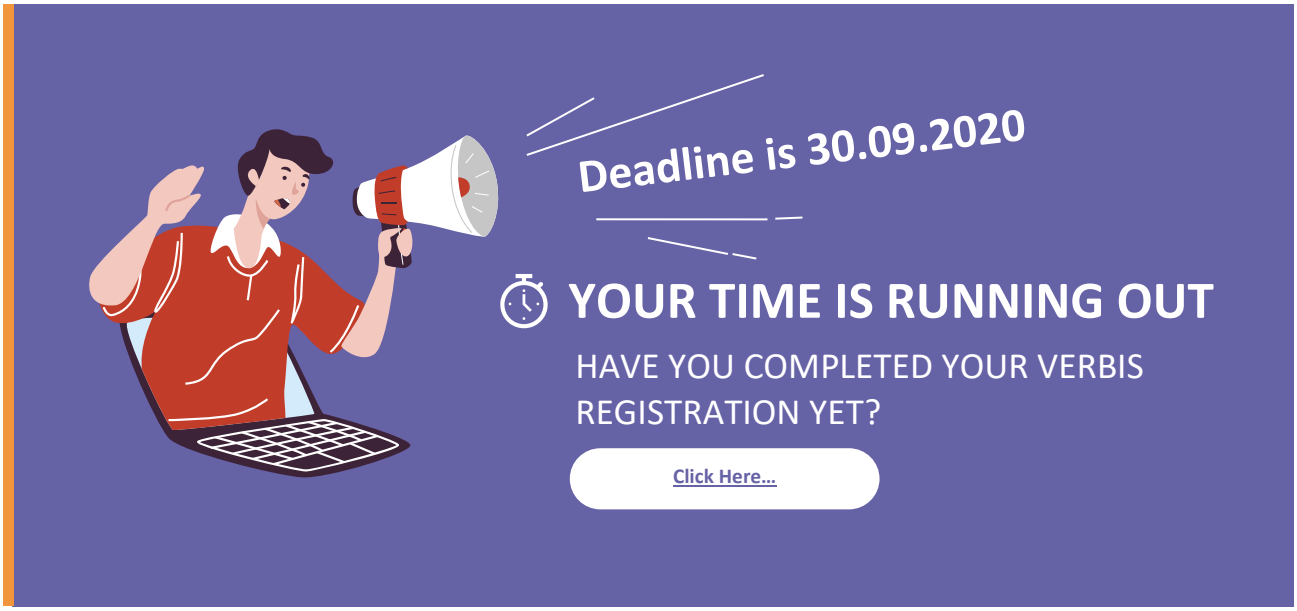
By synchronizing DLP products with classification systems, organizations can detect a content labeled as containing personal data from the "Personal Data" label in its field and prevent it from being taken outside of the organization. For example, restrictions may be imposed on forwarding e-mails labeled "Strictly Confidential Information" to unauthorized persons. Or, Or, in order to ensure physical document security, system restrictions can be imposed to prevent documents with "Confidential Information" label from being printed out and taken outside of the Organization.

In addition, if the person requests the deletion, destruction or anonymization of his personal data which are within the rights of the data subject, information classification and labeling processes facilitate carrying out the relevant transactions within the period specified in the law.

Finally, the destruction of personal data belonging to the Organization, the retention period of which has expired, is operated much more efficiently with information classification and labeling methods.

In this context, the most important process to protect and control the data within the Organization is to classify the information and to design what kind of data will be protected under which conditions.

Kübra Özkahraman | Quality Assurance & Training Responsible



LEGISLATION ANALYSIS

KVKK Art. 11 – Rights of the Data Subject

By applying to the data controller, every person has the right to;

a) learn whether or not their personal data are being processed,

b) request information in this respect, if personal data have been processed,

c) obtain information with regards to the purpose of processing the personal data and find out whether personal data is being used in line with such purpose,

ç) obtain information about the third parties with whom personal data were shared domestically or abroad,

d) request the correction of personal data that may be incompletely or inaccurately processed,

e) request the deletion or destruction of personal data within the scope of the provisions set forth in the Article 7,

f) request that the third parties to whom personal data are disclosed are informed about the transaction carried out pursuant to items (d) and (e),

g) object to the occurrence of a result which is to the detriment of the data subjects, by means of analyzing the personal data exclusively through automated systems,

ğ) request compensation in the event that losses are sustained as a result of unlawful processing of personal data.

***

The rights of the data subject are counted in the Article 11 of the Law No. 6698. These rights can only be used by the data subject; that is, except for the power of attorney, third parties other than the data subject cannot use these rights.

1. Learn whether or not their personal data are being processed: The data subject may wish to learn whether his personal data has been processed or not; whether processing continues after the retention period has expired. In such case, the data controller is obliged to provide correct information to the data subject.

2. Request information in this respect, if personal data have been processed: In addition to the information contained in the disclosure text and other information texts, the data subject may request information about the personal data processing activity by applying to the data controller who processes his personal data. In this case, the data controller is obliged to inform the person about the information requested within reasonable limits.

3. Obtain information with regards to the purpose of processing the personal data and find out whether personal data is being used in line with such purpose: The data subject must first be informed about the disclosure text and the purposes of processing his personal data. Additional information requests of the data subject regarding these purposes must be met by the data controller.

4. Obtain information about the third parties with whom personal data were shared domestically or abroad: As stated in the Communique On Principles And Procedures To Be Followed In Fulfillment Of The Disclosure Obligation, the data subject should be informed about the purpose of transferring personal data and the recipient groups to whom personal data will be transferred. In addition, the information about whether their data has been transferred abroad or not should also be provided to the data subject. For example, if the data subject requests information about the country where the data is transferred, the data controller is obliged to provide this information to the data subject based on his request, even if it is not included in the disclosure text.

5. Request the correction of personal data that may be incompletely or inaccurately processed: In the event that the data of the data subject is inaccurate or incomplete in the data controller's systems in any way, the data subject can apply to him with one of the effective application methods provided by the data controller. In this case, the request of the data subject must be answered by respecting the following conditions and must be fulfilled as soon as possible. For example, if a courier company enters the address information of the person incorrectly into their systems and as a result performs an incorrect activity, the data subject may request the data to be corrected by making a request. In such case, the data controller courier company is obliged to correct the mistake immediately. In addition, it should be kept in mind by the data controllers that such a situation is a serious data breach in the event that personal data reaches unauthorized persons, regardless of the request of the data subject or not.

6. Request the deletion or destruction of personal data within the scope of the provisions set forth in the Article 7: The data subject has the right to request the deletion or destruction of the personal data in the event that the data controller's purposes and legal reasons for processing personal data disappear. It should be kept in mind that the data controller must destruct the data without the request of the data subject in the event that the purposes and legal reasons for processing personal data disappear.

7. Request that the third parties to whom personal data are disclosed are informed about the transaction carried out pursuant to items (d) and (e): In the event that personal data are transferred to third parties, the data controller is obliged to notify the third parties to whom the personal data is transferred, if the data subject exercises his right to request correction of his personal data in case of incomplete or incorrect processing and/or to request the deletion or destruction of his personal data. Requests of the data subject must also be fulfilled by the data controller. wered by considering the balance between the purpose of the data processing activity and the interests of the data subject.

8. Object to the occurrence of a result which is to the detriment of the data subjects, by means of analyzing the personal data exclusively through automated systems: In the event of a result against the data subject as a result of the personal data processing activity, the data subject may object to the data processing activity that has consequences against him. In such case, the request of the data subject should be answered by considering the balance between the purpose of the data processing activity and the interests of the data subject.

9. Request compensation in the event that losses are sustained as a result of unlawful processing of personal data: In the event that the data subject suffers losses due to an illegal personal data processing activity, the loss of the data subject must be compensated upon his request. If this request is not met, the data subject can apply to the Authority on the grounds that his request is not fulfilled; may repeat the claim for compensation from the data controller at the general courts.

In addition, if the data subject wishes to exercise his rights listed in this article, pursuant to the Article 13 of the KVKK, the data controller should conclude the request within the shortest time possible based on the nature of the request and in any case within maximum 30 days following receipt of the request in writing or via other methods specified by the Board.

The response to be given by the data controller upon receipt of the request is whether the request is accepted or rejected including the justifications. The data controller should submit this response to the data subject in writing; provided that the response is affirmative, the data controller should fulfill the request of the data subject immediately.

In the event where the application is rejected, the response is found unsatisfactory, or there is a failure to respond to the application in due time, the data subject shall be entitled to file a complaint to the Board within 30 (thirty) days of receiving a response from the data controller or, in any case, within 60 (sixty) days following the application date. The application to the data controllers has been set forth in the "*Communiqué on Procedures and Principles for Application to the Data Controller*". You may access further information on the subject through our KVKK&GDPR May Newsletter via this link.

One of the points that the data controller should pay attention to regarding the application to be made to the data controller is not to bring an additional burden which is not envisaged in the Law or the Communiqué in order to provide identity confirmation while processing the application of the data subject. With its decision dated 01/10/2019 and numbered 2019/296, the Board has clearly stated its opinion on this issue by emphasizing that it does not comply with the rule of law and integrity, which is stated in the Article 6 of the Communiqué, that the prohibition of the right to make a proper application.

In addition, after applying to the data controller, an online complaint module has been created for the complaint to the Board in order to carry out the process described above. Complaint applications to the Board can be made easily by the data subjects through this module. You may access further information on the subject through our article via this link.

Şeyma Kaplan | Legal Consultant | Attorney

Prepared By

Hazal Özçelik

Kerem Akdağ

Kübra Özkahraman

Rabia Dağcı

Sevcan Livanur Sefer

Şeyma Kaplan

Şule Özcan

Suzan Tepe

Follow Us on Social Media...